WHITEPAPER

IEC 62443 EM SUBESTAÇÕES: CIBERSEGURANÇA, ZONAS, CONDUÍTES E ACESSO REMOTO

IEC 62443 aplicada a subestações: gestão de riscos, zonas e conduítes, segmentação OT, acesso remoto, hardening, vulnerabilidades, monitoramento, FAT, SAT e Owner’s Engineering.

A3A® Engenharia de Sistemas

SUMÁRIO

A digitalização das subestações ampliou a capacidade de proteção, controle, supervisão, teleassistência e diagnóstico, mas também aumentou a quantidade de ativos programáveis, interfaces de comunicação e acessos que precisam ser governados. Relés digitais, IEDs, UTRs, SSCLs, switches, gateways, servidores, estações de engenharia, sistemas SCADA e conexões com centros de operação formam uma infraestrutura de tecnologia operacional — OT — diretamente ligada ao processo elétrico.

Nesse ambiente, uma falha cibernética não se limita à perda de informação. Ela pode provocar perda de supervisão, indisponibilidade de telecomandos, alteração de ajustes, bloqueio de estações de engenharia, degradação de canais de comunicação ou apresentação de estados incorretos ao operador. A engenharia de cibersegurança precisa, portanto, preservar simultaneamente a segurança das pessoas, a integridade das funções, a disponibilidade da operação e a possibilidade de recuperação.

A **IEC 62443** oferece conceitos e estruturas para tratar a segurança de sistemas industriais de automação e controle ao longo do ciclo de vida. Em subestações, ela pode ser combinada com referências específicas de sistemas de potência, como a IEC 62351, com orientações de engenharia de redes da ABNT NBR 16932 e com práticas de segurança OT consolidadas pelo NIST SP 800-82.

Este artigo apresenta um método de aplicação desses conceitos a subestações de distribuição, transmissão e geração. O objetivo não é transformar a norma em uma lista genérica de equipamentos, mas mostrar como riscos, zonas, conduítes, acessos, hardening, monitoramento e testes se convertem em entregáveis de projeto e critérios de contratação.

1. POR QUE SUBESTAÇÕES EXIGEM UMA ABORDAGEM PRÓPRIA DE CIBERSEGURANÇA

Subestações combinam requisitos que normalmente não coexistem com a mesma intensidade em redes corporativas. Determinadas comunicações possuem restrições de latência e previsibilidade; ativos podem permanecer em operação por décadas; janelas de manutenção são limitadas; alterações precisam ser coordenadas com proteção, automação e operação; e falhas podem afetar a continuidade do fornecimento de energia.

Em TI corporativa, a confidencialidade pode ocupar posição central. Em OT, integridade e disponibilidade frequentemente recebem maior peso, com a segurança operacional como restrição superior. Isso não torna a confidencialidade irrelevante: diagramas, ajustes, topologias, credenciais e arquivos de configuração também são sensíveis. Significa que qualquer controle precisa ser analisado quanto ao efeito sobre o processo.

Uma solução de inspeção profunda, autenticação ou criptografia pode ser tecnicamente desejável, mas inadequada em um caminho de comunicação crítico se introduzir atraso, indisponibilidade ou comportamento não determinístico. A IEC 62443 reconhece esse conflito ao tratar o desempenho e a continuidade como parte do próprio problema de segurança.

A abordagem correta começa por quatro perguntas:

1. quais funções elétricas e operacionais precisam ser preservadas; 2. quais ativos e comunicações sustentam essas funções; 3. quais consequências podem resultar de alteração, indisponibilidade ou acesso indevido; 4. quais controles reduzem o risco sem comprometer proteção, controle e segurança operacional.

2. O QUE É A IEC 62443

A IEC 62443 é uma família de documentos voltada à cibersegurança de sistemas industriais de automação e controle. O trabalho original da ISA99 foi utilizado no desenvolvimento da série internacional, razão pela qual também são comuns as expressões **ISA/IEC 62443** e **ISA IEC 62443**.

A família distribui responsabilidades entre proprietários de ativos, prestadores de serviços, integradores e fabricantes. Em termos gerais, seus documentos tratam de:

A ABNT IEC/TS 62443-1-1:2023 disponível na base técnica da A3A estabelece conceitos fundamentais, como defesa em profundidade, ativos, ameaças, vulnerabilidades, zonas, conduítes e níveis de segurança. Ela não deve ser utilizada isoladamente como se contivesse todos os requisitos detalhados das demais partes da série.

Também é importante não apresentar a IEC 62443 como obrigação universal. Documentos técnicos ABNT são, em regra, voluntários. Eles podem se tornar exigíveis quando incorporados a contratos, padrões corporativos, editais, regulamentos ou outros instrumentos aplicáveis ao empreendimento.

3. REQUISITOS FUNDAMENTAIS DE SEGURANÇA INDUSTRIAL

A ABNT IEC/TS 62443-1-1 identifica sete grupos fundamentais de requisitos. Eles ajudam a verificar se o projeto cobre as dimensões essenciais da segurança.

Requisito fundamentalAplicação em uma subestaçãoControle de acessoRestringir quem ou qual sistema pode alcançar IEDs, servidores, switches, gateways e ferramentas de engenhariaControle de usoLimitar o que uma identidade autenticada pode visualizar,

alterar, comandar ou administrarIntegridade de dadosDetectar ou impedir alteração não autorizada de comandos, ajustes, arquivos, eventos e comunicaçõesConfidencialidade de dadosProteger informações sensíveis quando o risco ou o caminho de comunicação justificarRestrição de fluxo de dadosPermitir somente comunicações necessárias entre zonas e ativosResposta oportuna a eventosDetectar, registrar, comunicar e tratar violações ou anomalias em tempo compatível com o riscoDisponibilidade de recursosManter funções críticas e evitar que falhas ou ataques esgotem recursos necessários à operação

Esses requisitos não são uma lista de produtos. O controle de acesso, por exemplo, pode envolver identidade, regras de firewall, proteção física, política de fornecedores e aprovação operacional. A disponibilidade pode depender de redundância, alimentação CC, rotas independentes, backup e procedimentos de recuperação.

4. IEC 62443, IEC 62351, NIST 800-82 E ISO 27001

As referências se complementam, mas não possuem a mesma finalidade.

4.1. IEC 62443

Fornece uma estrutura para segurança de sistemas industriais de automação e controle, incluindo ciclo de vida, responsabilidades, risco, zonas, conduítes, requisitos de sistema e segurança de componentes.

4.2. IEC 62351

A série IEC 62351 trata da segurança de dados e comunicações utilizados no gerenciamento e intercâmbio de informações em sistemas de potência. A própria ABNT NBR 16932 indica essa série como referência para cibersegurança das comunicações e cita a parte dedicada à IEC 61850.

Enquanto a IEC 62443 ajuda a estruturar o programa e a arquitetura de segurança do ambiente OT, a IEC 62351 se aproxima dos mecanismos aplicáveis aos protocolos e intercâmbios do setor elétrico. A seleção de partes aplicáveis deve considerar os protocolos efetivamente utilizados e o suporte dos equipamentos.

4.3. NIST SP 800-82

O NIST SP 800-82 Rev. 3 é um guia de segurança OT que aborda governança, riscos, arquiteturas, segmentação, acesso remoto, monitoramento, fornecedores, vulnerabilidades, incidentes e recuperação. É uma referência de boas práticas, não um regulamento brasileiro.

O documento enfatiza que controles de TI precisam ser adaptados às restrições de desempenho, disponibilidade e segurança operacional da OT. Também recomenda uma equipe multidisciplinar, reunindo automação, operação, redes, TI, cibersegurança, segurança física, gestão e fornecedores quando necessário.

4.4. ISO/IEC 27001

A ISO/IEC 27001 fornece a estrutura de um sistema de gestão de segurança da informação. Ela é útil para governança, avaliação de riscos, responsabilidades, auditorias e melhoria contínua. A IEC 62443 adiciona especificidade para ambientes industriais e suas restrições operacionais.

Nenhuma dessas referências substitui os requisitos do proprietário do ativo, os procedimentos da concessionária, a filosofia de operação ou as condições contratuais do empreendimento.

5. SEGURANÇA NÃO É UM PROJETO COM DATA DE TÉRMINO

A IEC 62443 trata a segurança como um ciclo de vida. Uma arquitetura pode atender aos requisitos no momento do comissionamento e perder efetividade posteriormente por causa de novas vulnerabilidades, mudanças de configuração, obsolescência, acessos não revogados ou alteração das ameaças.

O ciclo precisa incluir:

Essa perspectiva é especialmente importante em subestações, onde a vida útil do ativo primário e dos sistemas de proteção pode superar o ciclo de suporte de sistemas operacionais, switches, servidores e componentes de software.

6. ATIVOS E FUNÇÕES CRÍTICAS DE UMA SUBESTAÇÃO

O inventário não deve começar apenas pelos endereços IP. É necessário relacionar ativos físicos, lógicos e humanos às funções que sustentam.

6.1. ATIVOS FÍSICOS E TECNOLÓGICOS

6.2. ATIVOS LÓGICOS

6.3. ATIVOS HUMANOS E ORGANIZACIONAIS

O comprometimento de uma estação de engenharia pode ser mais relevante do que a perda temporária de uma estação de consulta, porque a primeira pode alterar configurações de vários ativos. A criticidade precisa refletir função, autoridade e consequência.

7. INVENTÁRIO E CLASSIFICAÇÃO DOS ATIVOS OT

Um inventário útil para engenharia e segurança deve incluir, no mínimo:

CampoFinalidadeIdentificação e localizaçãoRelacionar o ativo ao bay, painel, sala, subestação ou centro de operaçãoFunçãoIndicar proteção, controle, supervisão, telecomunicação, vídeo ou gestãoFabricante e modeloApoiar suporte, vulnerabilidades, reposição e compatibilidadeHardware, firmware e softwareDeterminar situação de atualização e dependênciasInterfaces e endereçosMapear portas físicas, endereços IP, MAC, seriais e interfaces ópticasProtocolos e serviçosIdentificar MMS, GOOSE, SV, SNMP, NTP, PTP, DNP3, IEC 60870-5-104 e outrosZona e conduíteRelacionar o ativo à arquitetura de segurançaResponsávelDefinir proprietário técnico e autoridade de mudançaCriticidadeRegistrar impacto da perda de integridade, disponibilidade ou controleSuporte e fim de vidaPlanejar atualização, estoque, substituição e controles compensatóriosBackup e restauraçãoInformar onde está a configuração e como recuperá-la

Descoberta automática pode auxiliar, mas ferramentas ativas precisam ser utilizadas com cautela. O NIST registra que varreduras e testes inadequados já causaram interrupções em redes de controle. Em ambientes em operação, levantamento passivo, documentação existente, consultas aos equipamentos e janelas controladas tendem a ser mais seguros.

8. ANÁLISE DE RISCOS CIBERNÉTICOS

A análise de riscos deve relacionar ativos, ameaças, vulnerabilidades, consequências e controles. Não basta importar uma matriz de TI e trocar o nome dos servidores.

Em subestações, as consequências podem incluir:

Uma avaliação prática pode seguir o ciclo:

1. definir escopo, fronteiras e funções críticas; 2. inventariar ativos e comunicações; 3. identificar ameaças e vulnerabilidades; 4. avaliar consequências físicas, operacionais e digitais; 5. estimar risco inicial; 6. selecionar controles técnicos, administrativos e físicos; 7. avaliar impacto dos controles sobre a operação; 8. registrar risco residual e autoridade de aceitação; 9. monitorar mudanças e reavaliar periodicamente.

A resposta pode envolver evitar, reduzir, compartilhar, transferir ou aceitar o risco. A aceitação precisa ser explícita e rastreável, principalmente quando a correção depende de uma futura janela de desligamento ou substituição do ativo.

9. AMEAÇAS RELEVANTES PARA SUBESTAÇÕES

A segurança não deve considerar apenas invasores externos. A IEC 62443 e o NIST tratam ameaças intencionais, acidentais, estruturais e ambientais.

OrigemExemplosAdversarialacesso indevido, malware, manipulação de comandos, falsificação de dados, negação de serviço e abuso de credenciaisInternaalteração não autorizada, uso excessivo de privilégios, remoção de logs ou conexão de dispositivo não aprovadoAcidentalerro de configuração, aplicação de patch incompatível, comando na instalação errada ou uso de ferramenta inadequadaEstruturalfalha de hardware, fonte, switch, software, armazenamento, sincronismo ou comunicaçãoAmbientalsurtos, interferência eletromagnética, perda de climatização, incêndio, inundação ou falha prolongada de energiaCadeia de suprimentoscomponente comprometido, software sem suporte, atualização insegura ou acesso excessivo do fornecedor

A arquitetura deve responder também a erros e falhas não maliciosas. Um controle que protege contra invasão, mas cria um ponto único de falha, pode reduzir a segurança global da operação.

10. ZONAS E CONDUÍTES

Zonas e conduítes são conceitos centrais da IEC 62443.

Uma **zona de segurança** agrupa ativos físicos, lógicos ou de aplicação que compartilham requisitos de segurança. Ela possui fronteira, política, responsáveis e critérios de acesso. Pode ser física, como uma sala de telecomunicações, ou lógica, como um conjunto de servidores e IEDs separados por função.

Um **conduíte** agrupa comunicações e mecanismos que permitem o fluxo de informações dentro de uma zona ou entre zonas. Um conduíte pode incluir enlaces, switches, roteadores, firewalls, gateways, VPNs e regras que protegem os canais transportados.

A definição deve partir da função e do risco, não apenas da topologia existente.

ElementoPerguntas de projetoAtivos da zonaQuais dispositivos, aplicações e pessoas pertencem ao agrupamento?FunçãoQue processo ou serviço a zona sustenta?FronteiraOnde começa e termina a responsabilidade e o controle?RiscoQual a consequência de comprometimento ou indisponibilidade?FluxosCom quais zonas a comunicação é realmente necessária?ControlesComo identidade, integridade, disponibilidade e restrição de fluxo serão implementadas?GestãoQuem aprova mudanças e quem responde pelos ativos?MonitoramentoQuais eventos e indicadores demonstram a condição da zona?

Uma VLAN não constitui, isoladamente, uma zona de segurança completa. Ela pode colaborar com a separação lógica, mas precisa ser combinada com controles de fluxo, proteção de portas, gestão de configuração, monitoração, regras de acesso e documentação.

11. ARQUITETURA DE REFERÊNCIA PARA SUBESTAÇÕES

Cada concessionária ou agente pode adotar uma arquitetura corporativa de referência e detalhá-la por família de subestação. O modelo precisa refletir a realidade operacional, e não apenas um desenho genérico baseado em níveis.

Uma decomposição possível é apresentada a seguir.

ZonaAtivos e funções típicasConsiderações principaisProcessosensores, atuadores, merging units e interfaces primáriasintegridade, disponibilidade, latência e acesso físicoProteção e controlerelés, IEDs, unidades de bay e intertravamentosdesempenho determinístico, independência e mudança controladaSupervisão localUTR, SSCL, gateways, IHM e servidores locaisdisponibilidade, lista de pontos, comandos e logsEstação de engenhariaferramentas, notebooks e arquivos de configuraçãoacesso privilegiado, integridade e rastreabilidadeTelecomunicações operacionaisswitches, roteadores, multiplexadores e WANredundância, rotas, gestão e supervisãoTeleproteçãorelés, equipamentos e canais dedicados ou lógicosbaixa latência, independência e testes ponta a pontaVídeo operativocâmeras, VMS, gravação e integrações com eventosseparação de tráfego, disponibilidade e acesso controladoSegurança patrimonialCFTV, acesso, perímetro e intrusãoimpedir que sistemas de segurança criem caminho para a OTDMZ OTjump server, proxy, repositório e transferência controladaimpedir comunicação direta entre rede corporativa e OT críticaCentro de operaçãoSCADA, históricos, estações e serviços de gestãoidentidade, disponibilidade, segregação e continuidadeRede corporativaaplicações administrativas e

usuários geraisnão deve alcançar diretamente ativos de níveis operacionais inferioresAcesso remotoVPN, bastion, autenticação e registro de sessõesaprovação, duração limitada, menor privilégio e revogação

A lista não é universal. Uma instalação pequena pode combinar funções; uma operação de maior criticidade pode subdividir proteção principal e alternada, separar estações de engenharia por domínio ou criar zonas distintas para sincronismo e gestão.

12. SEGMENTAÇÃO ENTRE PROTEÇÃO, CONTROLE, SCADA, VÍDEO E GESTÃO

A segmentação deve impedir que uma falha ou comprometimento em um sistema menos crítico se propague livremente para funções de proteção e controle.

Algumas separações que merecem análise são:

A ABNT NBR 16932 fornece orientações de engenharia para redes IEC 61850, incluindo topologias, redundância, VLAN, multicast, desempenho, sincronismo, gerenciamento e testes. A própria norma informa que não detalha cibersegurança. Por isso, seu uso deve ser combinado com uma arquitetura de segurança baseada em risco.

Separação lógica pode ser adequada em certas aplicações, desde que o risco, o desempenho e as falhas comuns sejam analisados. Proteção principal e alternada em VLANs diferentes, mas nos mesmos switches, fontes e enlaces, continuam sujeitas a dependências compartilhadas.

13. MATRIZ DE FLUXOS AUTORIZADOS

Antes de configurar firewalls e ACLs, deve ser produzida uma matriz de comunicação. Ela transforma a arquitetura em requisitos verificáveis.

OrigemDestinoServiço ou protocoloDireçãoFinalidadeCriticidadeResponsávelIED de baySSCLMMSconforme arquiteturasupervisão e controlealtaautomaçãoIEDIEDGOOSEmulticast localintertravamento ou proteçãocríticaproteçãoRelógioIEDs e switchesPTP/NTP/IRIG-Bdistribuiçãosincronismoaltaautomação/telecomSSCLCentro de operaçãoprotocolo de telecontrolebidirecional controladodados e telecomandosaltaoperaçãoEstação de engenhariaIEDprotocolo de gestãosessão autorizadaparametrizaçãocríticaproteção/automaçãoDispositivo OTservidor de logssyslog ou mecanismo suportadosaídaauditoriamédia/altacibersegurança

A política recomendada é negar por padrão e permitir somente o necessário. Regras de saída também precisam ser controladas. Um ativo comprometido pode utilizar comunicações de saída para movimentação lateral, comando e controle ou exfiltração.

14. DMZ OT E COMUNICAÇÃO COM A REDE CORPORATIVA

Quando existe necessidade de integração entre OT e TI, a comunicação direta entre a rede corporativa e os níveis críticos deve ser evitada. Uma DMZ OT pode hospedar serviços intermediários, como:

A DMZ não deve ser apenas uma VLAN com nome diferente. Ela precisa possuir fronteiras controladas, políticas distintas, regras mínimas, monitoramento e procedimentos de administração.

Em casos nos quais o fluxo precisa ocorrer somente da OT para ambientes superiores, gateways unidirecionais podem ser considerados. A decisão depende dos serviços requeridos, da necessidade de comandos ou manutenção e da análise de risco.

15. IDENTIDADES, PERFIS E MENOR PRIVILÉGIO

Acesso a ativos OT deve ser concedido com base em função, necessidade e período. Operadores, engenheiros, administradores, auditores e fornecedores não precisam das mesmas permissões.

O projeto deve definir:

Contas compartilhadas reduzem a rastreabilidade. Quando um equipamento legado não permite identidades individuais, controles compensatórios podem incluir cofre de senhas, registro de retirada, supervisão da sessão, aprovação prévia e correlação com ordem de serviço.

A autenticação corporativa não deve ser aplicada automaticamente a todos os níveis. Uma dependência direta da rede OT em serviços corporativos pode comprometer a disponibilidade. A arquitetura precisa decidir quais serviços serão locais, replicados ou isolados.

16. ESTAÇÕES DE ENGENHARIA

A estação de engenharia possui autoridade elevada porque pode alterar ajustes, lógicas, arquivos SCL, configurações de rede e parâmetros de dispositivos. Ela deve ser tratada como ativo crítico, não como notebook convencional de manutenção.

Controles possíveis incluem:

Quando notebooks de fornecedores são permitidos, o contrato precisa definir requisitos mínimos, validação, ferramentas autorizadas, acesso à internet, proteção contra malware e procedimento de quarentena.

17. ACESSO REMOTO DE OPERADORES E FORNECEDORES

O acesso remoto atravessa a fronteira física da subestação. Uma VPN, isoladamente, não resolve identidade, autorização, duração, destino, registro e revogação.

Uma arquitetura robusta pode incluir:

1. solicitação vinculada a chamado ou ordem de serviço; 2. aprovação operacional e técnica; 3. autenticação multifator na entrada remota; 4. acesso a jump server na DMZ OT; 5. autorização somente para ativos e protocolos necessários; 6. janela de tempo definida; 7. monitoramento e registro da sessão; 8. encerramento automático ao fim da atividade; 9. validação da configuração alterada; 10. revogação imediata após conclusão ou término contratual.

Conexões permanentes de fabricantes, modems esquecidos, softwares de suporte não inventariados e regras amplas de VPN constituem riscos recorrentes. O inventário deve incluir todos os caminhos remotos, inclusive soluções de nuvem, links celulares e ferramentas embutidas em equipamentos.

A manutenção remota também precisa de modo degradado. A subestação não pode depender da disponibilidade do acesso do fornecedor para executar funções essenciais ou restaurar uma configuração básica.

18. HARDENING DE IEDS, RELÉS, SWITCHES E GATEWAYS

Hardening é a definição e aplicação de uma configuração de referência que reduz a superfície de ataque sem impedir a função operacional.

18.1. IEDS E RELÉS

18.2. SWITCHES E ROTEADORES

18.3. SERVIDORES E ESTAÇÕES

Uma baseline precisa identificar quais requisitos são obrigatórios, recomendados ou não aplicáveis. Exceções devem possuir justificativa, risco, controle compensatório e aprovação.

19. GESTÃO DE FIRMWARE, PATCHES E VULNERABILIDADES

Atualizar imediatamente qualquer ativo pode ser tão arriscado quanto nunca atualizar. O processo deve combinar inteligência de vulnerabilidades, análise de aplicabilidade e validação operacional.

Etapas recomendadas:

1. receber avisos de fabricantes, CISA, bases de vulnerabilidade e fontes setoriais; 2. identificar modelos, versões e ativos afetados; 3. avaliar exposição, função, consequência e existência de exploração; 4. consultar compatibilidade e dependências; 5. testar em ambiente representativo; 6. planejar janela, backup e retorno; 7. aplicar e validar funções; 8. registrar evidências e atualizar inventário; 9. implementar controle compensatório quando a correção não puder ser aplicada.

Controles compensatórios podem envolver segmentação adicional, restrição de acesso, bloqueio de serviço vulnerável, monitoração específica ou substituição planejada. Eles não devem se tornar desculpa permanente para manter ativos sem suporte.

O programa também precisa tratar fim de vida. Fabricantes e integradores devem informar períodos de suporte, política de vulnerabilidades, disponibilidade de firmware e requisitos de atualização.

20. CERTIFICADOS, CHAVES E SINCRONISMO

Certificados e chaves podem autenticar dispositivos, usuários e comunicações, mas introduzem uma infraestrutura que precisa ser operada.

O projeto deve definir:

O sincronismo também sustenta eventos, registros e investigação. Fontes de tempo, caminhos principal e alternativo, holdover, alarmes e segurança da distribuição precisam ser documentados. A alteração indevida do tempo pode prejudicar correlação de eventos e rastreabilidade.

21. LOGS, MONITORAMENTO E DETECÇÃO

A monitoração deve combinar contexto operacional e cibernético. Em redes OT, o tráfego tende a ser mais previsível que em redes corporativas, o que favorece a criação de baselines.

Fontes possíveis incluem:

Eventos relevantes:

A coleta passiva por TAP ou SPAN costuma ser preferível como ponto inicial. Respostas automáticas de IPS precisam ser cuidadosamente avaliadas, porque um bloqueio incorreto pode afetar comunicações críticas.

Integração com SIEM ou SOC é possível, mas os casos de uso devem considerar a semântica da OT. Uma rajada GOOSE legítima, uma comutação de PRP ou uma sequência de eventos operacionais não deve ser interpretada sem contexto.

22. BACKUP, RESTAURAÇÃO E CONTINUIDADE

Backup precisa abranger mais que arquivos de servidor. A recuperação pode depender de:

As cópias precisam ser protegidas contra alteração e indisponibilidade. Ao menos uma parcela deve permanecer separada do ambiente operacional para resistir a incidentes destrutivos.

A restauração deve ser testada. O teste precisa responder:

Continuidade também envolve operação degradada. Procedimentos precisam indicar como a subestação será operada durante perda de SCADA, WAN, servidor, sincronismo, estação de engenharia ou parte da monitoração cibernética.

23. RESPOSTA A INCIDENTES EM AMBIENTES OT

O plano de resposta deve ser elaborado antes do incidente. A contenção de TI baseada em desligar ou isolar imediatamente um equipamento pode ser inadequada quando o ativo sustenta proteção, controle ou segurança.

O procedimento deve definir:

Cenários úteis para exercícios incluem:

Exercícios de mesa permitem verificar decisões e responsabilidades sem impactar a instalação. Testes técnicos precisam ser planejados para não interromper funções ativas.

24. SEGURANÇA FÍSICA E CIBERSEGURANÇA

A fronteira cibernética pode ser ultrapassada fisicamente. Portas de switch, interfaces seriais, USB, painéis, racks, caixas de emenda e equipamentos em locais remotos precisam de proteção proporcional à criticidade.

A integração com controle de acesso, intrusão e CFTV pode ajudar a correlacionar:

Os próprios sistemas de segurança física são ativos conectados. Câmeras, controladoras e painéis não devem criar uma ponte não controlada para redes de automação. Vídeo operativo e segurança patrimonial devem possuir fluxos e zonas definidos.

25. SEGURANÇA DE FORNECEDORES E CADEIA DE SUPRIMENTOS

Subestações dependem de fabricantes, integradores, desenvolvedores e prestadores de manutenção. O risco não termina na entrega do equipamento.

Requisitos contratuais podem incluir:

Um produto certificado ou com recursos de segurança não garante, sozinho, que a instalação alcançará o nível pretendido. A segurança resulta da combinação entre capacidades do componente, arquitetura, configuração, processos e operação.

26. PROJETO E DOCUMENTAÇÃO DE CIBERSEGURANÇA OT

A contratação precisa resultar em documentos utilizáveis pela implantação, operação e fiscalização.

Entre os entregáveis possíveis estão:

O projeto deve identificar claramente o que pertence à concessionária, ao integrador de automação, ao fornecedor de telecomunicações, ao fabricante de relés e à equipe de cibersegurança. Interfaces indefinidas tendem a gerar lacunas.

27. MODERNIZAÇÃO DE SUBESTAÇÕES EXISTENTES

Em instalações existentes, a implantação deve começar por diagnóstico e plano de transição. Equipamentos legados podem não suportar autenticação individual, criptografia, logs ou firmware atual.

A modernização precisa considerar:

A segmentação pode ser implantada progressivamente, começando por fronteiras críticas, acessos remotos e caminhos entre TI e OT. O objetivo é reduzir risco sem criar uma transformação inviável ou uma arquitetura paralela impossível de manter.

28. FAT, SAT E COMISSIONAMENTO CIBERNÉTICO

Controles de segurança precisam ser testados como parte do sistema. O **FAT** pode verificar configurações, perfis, fluxos, hardening, logs, backups e comportamento de componentes antes da instalação. O **SAT** valida a arquitetura real, incluindo enlaces, endereços, regras, integrações e condições de campo.

Uma matriz de testes pode incluir:

DomínioVerificaçãoInventáriomodelo, versão, endereço, função e responsável conferem com o projetoZonasativos estão conectados às zonas previstas e não existem caminhos alternativosFluxossomente portas, protocolos, origens e destinos aprovados são permitidosIdentidadesperfis, contas administrativas, contas técnicas e revogações funcionamAcesso remotoMFA, aprovação, jump server, limitação temporal e logs são comprovadosHardeningserviços desnecessários, credenciais padrão e portas não utilizadas foram tratadosRedundânciafalhas de links, equipamentos e fontes não eliminam funções críticasDesempenhocontroles não degradam GOOSE, SV, teleproteção, SCADA ou sincronismo além do permitidoMonitoramentoeventos são gerados, transportados, sincronizados e interpretados corretamenteBackupconfigurações são exportadas, protegidas e restauradas em ambiente controladoIncidentesprocedimentos, contatos e operação degradada são exercitadosDocumentaçãodiagramas, matrizes, configurações e relatórios refletem a instalação final

Testes ativos, varreduras e simulações precisam ser autorizados e avaliados quanto ao risco. Em produção, ferramentas inadequadas podem travar controladores ou degradar comunicações.

29. CRITÉRIOS DE ACEITE E DOSSIÊ TÉCNICO

Cada requisito deve estar associado a método, resultado esperado, tolerância e evidência. Declarações como “rede segmentada” ou “acesso seguro” são insuficientes sem demonstração.

O dossiê pode reunir:

Pendências de cibersegurança precisam possuir responsável, prazo, impacto e controle temporário. A energização ou entrada em operação não deveria apagar a rastreabilidade dessas pendências.

30. OWNER'S ENGINEERING EM PROGRAMAS DE SUBESTAÇÕES

Em programas com várias subestações e fornecedores, o Owner's Engineering pode atuar na governança das interfaces e na verificação independente dos requisitos.

Atividades possíveis:

Essa função é particularmente útil quando cada fornecedor comprova apenas seu equipamento, mas ninguém demonstra o comportamento integrado da subestação e do centro de operação.

31. INDICADORES PARA OPERAÇÃO CONTÍNUA

Após o comissionamento, indicadores ajudam a demonstrar se o nível de segurança está sendo mantido.

O indicador não deve incentivar ações inseguras. Uma meta de aplicação rápida de patches, por exemplo, precisa considerar teste, janela e impacto operacional.

32. ERROS COMUNS

32.1. TRATAR A IEC 62443 COMO CHECKLIST DE EQUIPAMENTOS

A norma estrutura risco, responsabilidades, arquitetura e ciclo de vida. Comprar firewall ou NAC não substitui inventário, fluxos, políticas e testes.

32.2. CRIAR VLANS SEM CONTROLAR COMUNICAÇÕES

VLANs ajudam na organização e segmentação lógica, mas não garantem, sozinhas, restrição de fluxo, identidade ou monitoração.

32.3. APLICAR PRÁTICAS DE TI SEM AVALIAR A OPERAÇÃO

Varreduras, patches, IPS e autenticação podem introduzir indisponibilidade ou latência. Cada controle precisa ser testado no contexto da função.

32.4. CONECTAR SISTEMAS DE APOIO DIRETAMENTE À REDE CRÍTICA

Vídeo, acesso, manutenção, impressão, antivírus, historização e serviços corporativos podem criar caminhos não planejados.

32.5. MANTER ACESSO PERMANENTE DE FORNECEDORES

Acesso sem aprovação, duração, registro e revogação amplia a superfície de ataque e reduz a responsabilização.

32.6. NÃO CONHECER OS ATIVOS EXISTENTES

Sem modelo, versão, firmware, função e responsável, não é possível avaliar vulnerabilidade, suporte ou impacto.

32.7. CONFUNDIR REDUNDÂNCIA COM INDEPENDÊNCIA

Dois sistemas que compartilham switch, fonte, cabo, servidor ou credencial podem falhar simultaneamente.

32.8. TESTAR APENAS A CONFIGURAÇÃO NOMINAL

O aceite precisa incluir perda de link, falha de autenticação, indisponibilidade de serviço, restauração, comutação e operação degradada.

32.9. ENCERRAR O PROGRAMA APÓS A IMPLANTAÇÃO

O nível alcançado diminui com o tempo. Auditoria, vulnerabilidades, mudanças, treinamento e revalidação precisam continuar.

33. COMO CONTRATAR UM PROJETO DE CIBERSEGURANÇA PARA SUBESTAÇÕES

O termo de referência deve informar:

Propostas devem ser comparadas pelo método e pelos produtos de engenharia, não apenas pela quantidade de equipamentos de segurança. O contratante precisa saber quem realizará o levantamento, como riscos serão avaliados, quais documentos serão produzidos e como os controles serão testados.

34. CONCLUSÃO

Aplicar a IEC 62443 em subestações significa transformar riscos operacionais em decisões de arquitetura, responsabilidades, controles e evidências. O resultado não é uma rede isolada de forma indiscriminada, mas uma infraestrutura na qual cada ativo é conhecido, cada comunicação possui finalidade, cada acesso possui autoridade e cada mudança pode ser rastreada.

A segurança precisa preservar proteção, controle, telecomunicações e operação. Por isso, o projeto deve integrar engenharia elétrica, automação, redes, cibersegurança, segurança física e operação desde a definição dos requisitos até o comissionamento.

Zonas e conduítes oferecem uma linguagem para organizar essa arquitetura. Inventário, matriz de fluxos, acesso remoto controlado, hardening, monitoramento, recuperação e testes completam o ciclo. A manutenção contínua garante que o nível alcançado não se perca com vulnerabilidades, mudanças e obsolescência.

[1] ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS. ABNT IEC/TS 62443-1-1:2023 — Segurança para sistemas de automação e controle industriais — Parte 1-1: Terminologia, conceitos e modelos.

[2] NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY. NIST SP 800-82 Rev. 3 — Guide to Operational Technology (OT) Security. 2023.

[3] ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS. ABNT NBR 16932:2020 — Redes e sistemas de comunicação para automação de sistemas de potência — Orientações sobre engenharia de rede.

[4] ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS. ABNT NBR IEC 61850-10:2018 — Redes e sistemas de comunicação para automação de sistemas de potência — Parte 10: Ensaios de conformidade.

[5] NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY. NIST CSWP 28 — Security Segmentation in a Small Manufacturing Environment.

O que é a IEC 62443? É uma família de documentos para cibersegurança de sistemas industriais de automação e controle. Ela trata de conceitos, programas de segurança, avaliação de riscos, requisitos de sistemas, prestadores de serviços e componentes.**A IEC 62443 é obrigatória em todas as subestações?** Não de forma universal. Documentos técnicos são normalmente voluntários, mas podem se tornar requisitos quando incorporados a contratos, padrões corporativos, editais, regulamentos ou outros

instrumentos aplicáveis.**O que são zonas e conduítes?** Uma zona agrupa ativos que compartilham requisitos de segurança. Um conduíte agrupa e protege as comunicações dentro de uma zona ou entre zonas, incluindo canais, equipamentos, regras e mecanismos de controle.**Uma VLAN é suficiente para criar uma zona de segurança?** Não. A VLAN pode colaborar com a separação lógica, mas a zona também precisa de fronteira, política, controle de fluxos, gestão de acesso, monitoramento, responsáveis e critérios de teste.**Qual a diferença entre IEC 62443 e IEC 62351?** A IEC 62443 estrutura a segurança de sistemas industriais, seu ciclo de vida, riscos, zonas e requisitos. A IEC 62351 se concentra na segurança de dados e comunicações utilizados em sistemas de potência. Elas são complementares.**Como deve funcionar o acesso remoto a uma subestação?** O acesso deve ser aprovado, autenticado com mecanismos fortes, limitado aos ativos necessários, preferencialmente intermediado por jump server ou bastion, registrado, temporário e revogado ao término da atividade.**É possível aplicar patches imediatamente em ativos OT?** Nem sempre. Patches precisam ser avaliados e testados quanto à compatibilidade, desempenho e segurança operacional. Quando não podem ser aplicados, devem ser adotados controles compensatórios e um plano de correção ou substituição.**Como monitorar uma rede OT sem prejudicar a operação?** A monitoração passiva por TAP ou SPAN costuma ser o ponto inicial mais seguro. Ferramentas ativas e respostas automáticas precisam ser avaliadas e testadas para não degradar comunicações críticas.**CFTV e controle de acesso podem compartilhar a rede de automação?** O compartilhamento não deve ser presumido. Vídeo, segurança física e automação possuem requisitos diferentes e devem ser separados por zonas e fluxos controlados conforme a análise de risco.**O que deve ser testado no FAT e no SAT de cibersegurança?** Devem ser verificados inventário, zonas, fluxos, perfis, acesso remoto, hardening, logs, redundância, desempenho, backup, recuperação, falhas e aderência da documentação à instalação real.**Qual o papel do Owner's Engineering em cibersegurança OT?** O Owner's Engineering pode revisar requisitos, coordenar interfaces, analisar propostas, fiscalizar fornecedores, acompanhar testes, controlar pendências e consolidar evidências para o aceite técnico.**Quais documentos compõem um projeto de cibersegurança para subestações?** Entre os principais estão inventário, matriz de riscos, arquitetura, mapa de zonas e conduítes, matriz de fluxos, perfis de acesso, baseline de hardening, política de acesso remoto, plano de vulnerabilidades, monitoramento, backup, incidentes e testes.

Soluções

Serviços de engenharia

Materiais técnicos complementares

Sobre a A3A Engenharia de Sistemas

Com 30 anos de história, a A3A Engenharia de Sistemas se consolidou como referência em serviços de Engenharia, oferecendo soluções integradas de Telecomunicações, Segurança Eletrônica, Segurança Digital e Instalações Elétricas.

A empresa atua em todas as etapas do ciclo de Engenharia, desde a elaboração de projetos e consultoria técnica até a implantação, manutenção e retrofit de sistemas, sempre em conformidade com as normas técnicas e melhores práticas do setor.

A3A® Engenharia de Sistemas